FIG. 1

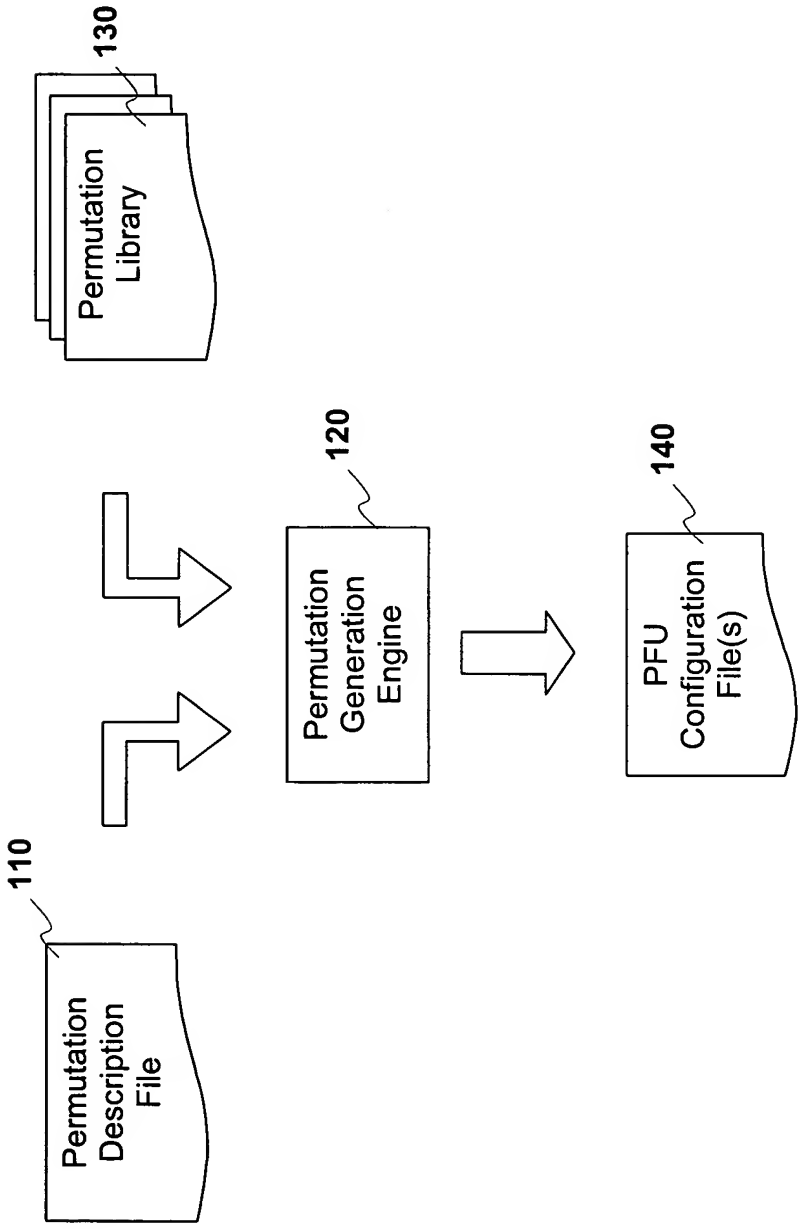
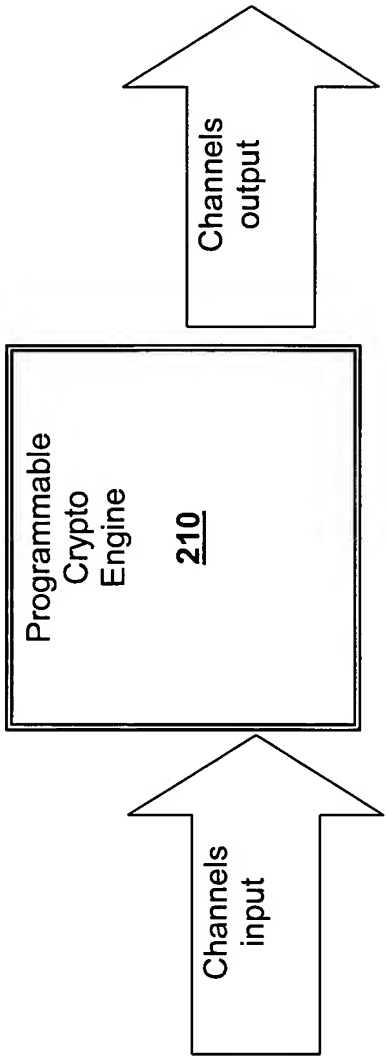

130
Permutation Library
120
Permutation Generation Engine
140
PFU Configuration File(s)
110
Permutation Description File

FIG. 2A


Channels output
Programmable Crypto Engine
210
Channels input

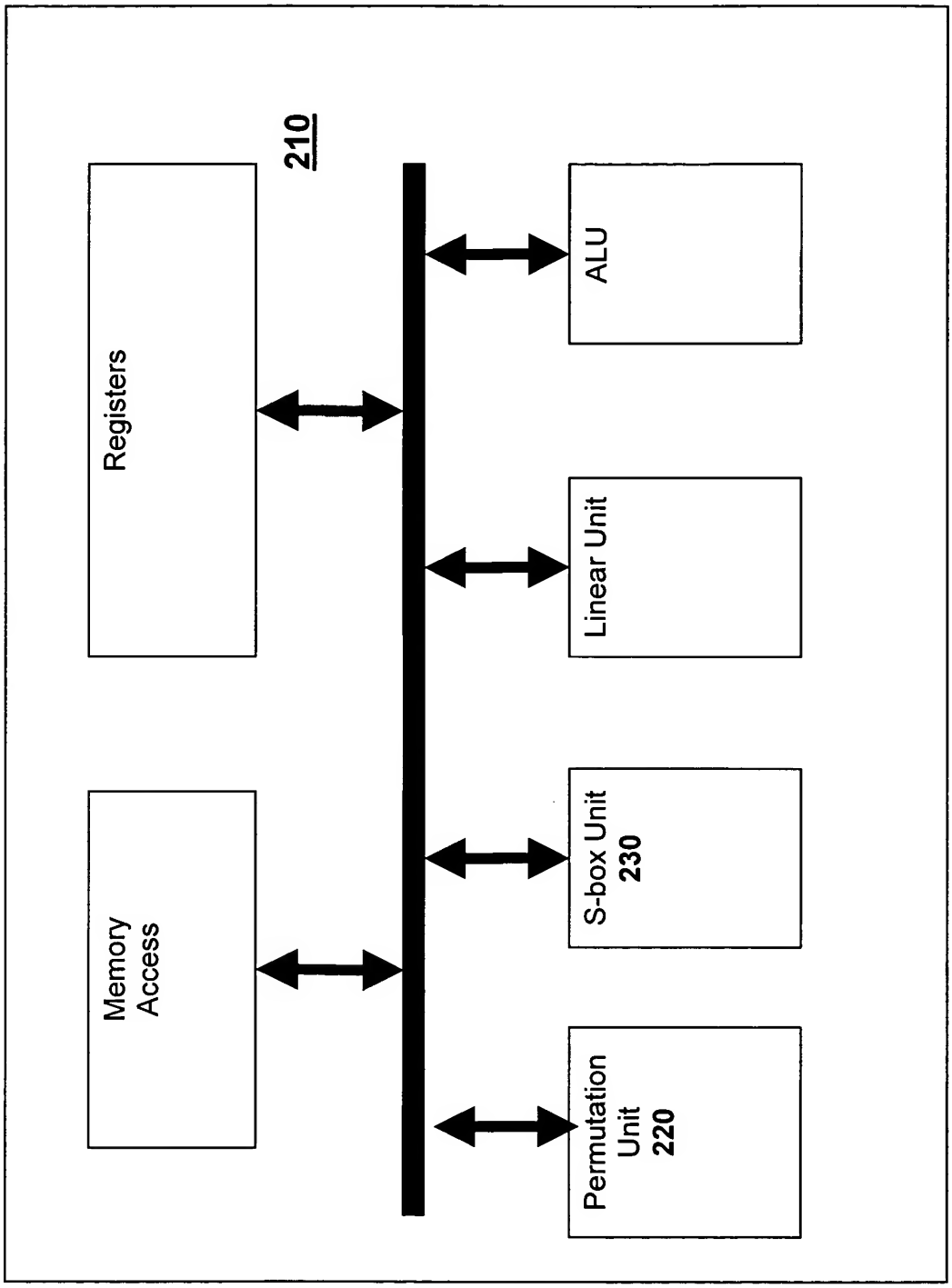
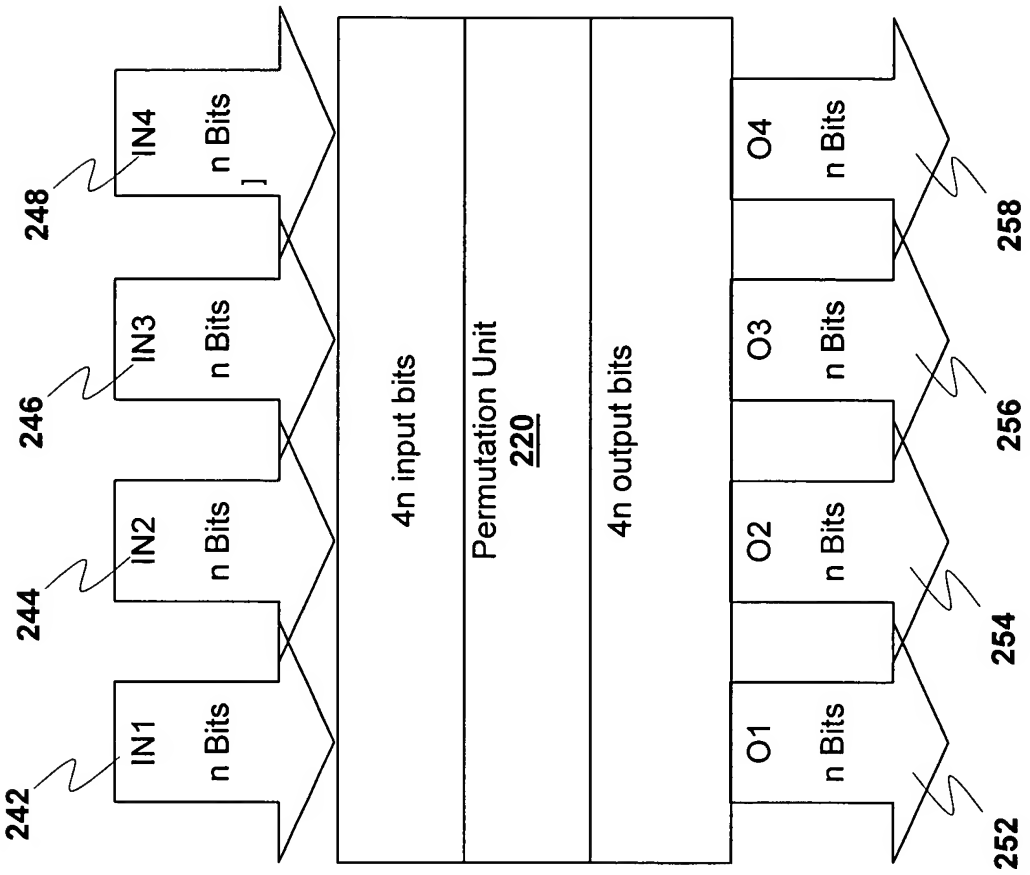

210
Registers
ALU
Linear Unit
Memory Access
S-box Unit 230
Permutation Unit 220

FIG. 2B

FIG. 2C


242
IN1
n Bits
244
IN2
n Bits
246
IN3
n Bits
248
IN4
n Bits
4n input bits
Permutation Unit
220
4n output bits
O1
n Bits
252
O2
n Bits
254
O3
n Bits
256
O4
n Bits
258

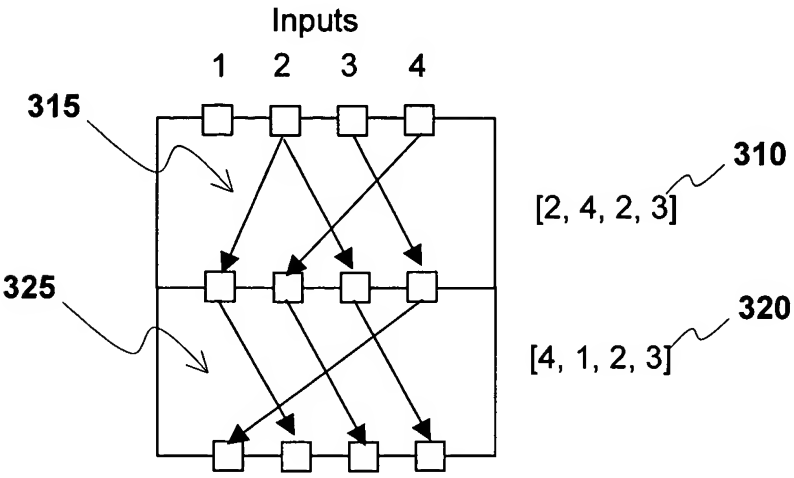


FIG. 3A

Output Number	(1	2	3	4)
Original Input Source	3	2	4	2

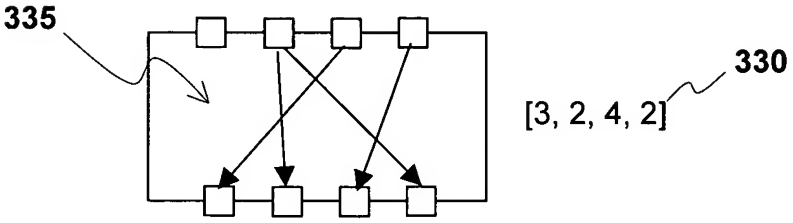


FIG. 3B

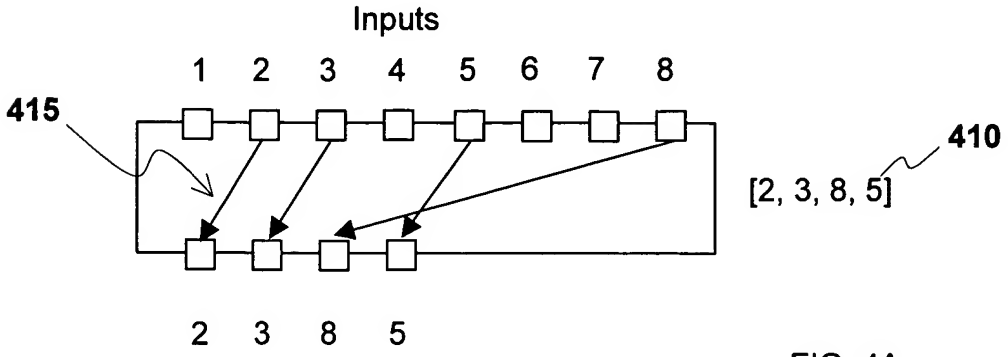


FIG. 4A

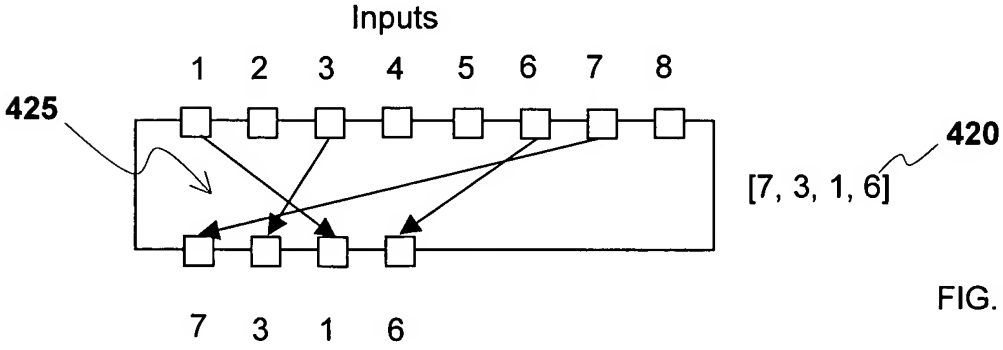


FIG. 4B

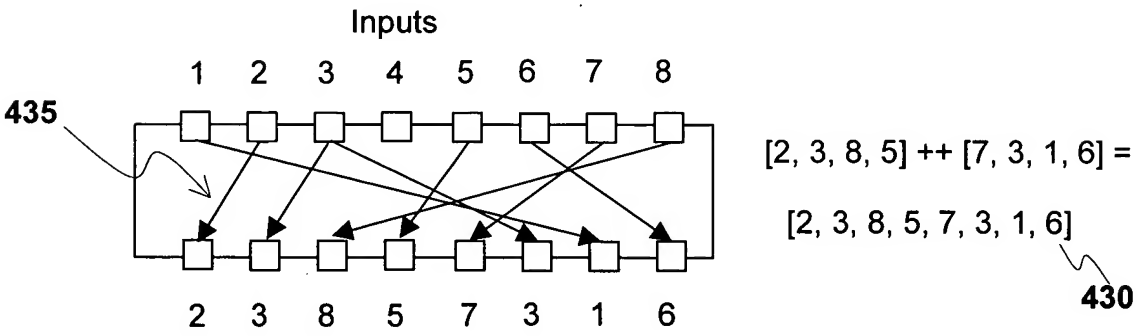


FIG. 4C

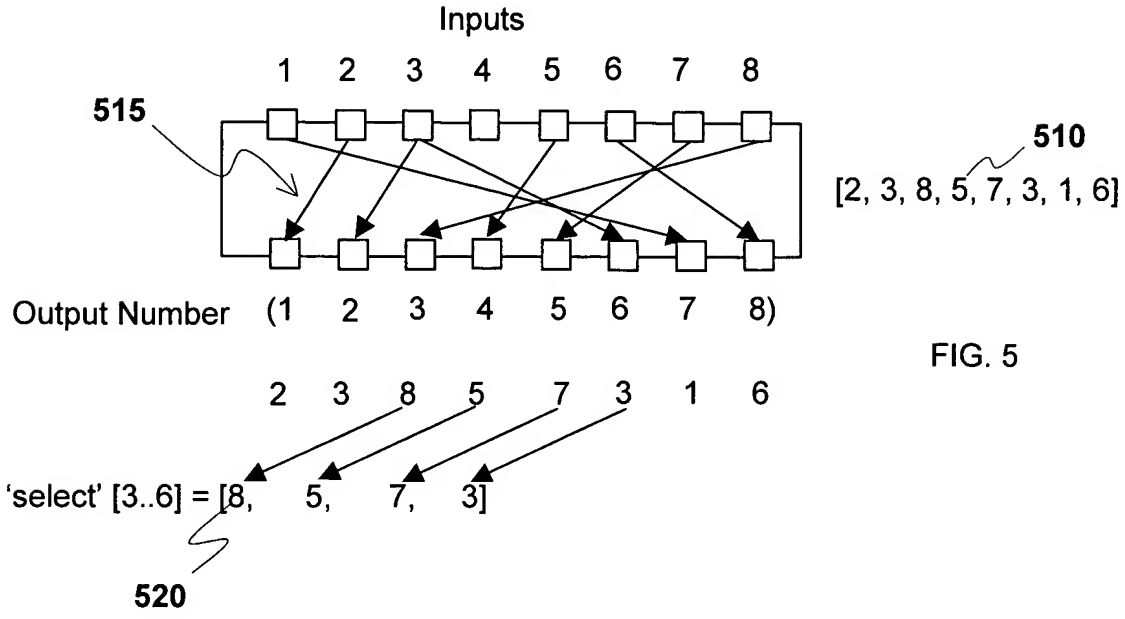

Inputs
1 2 3 4 5 6 7 8
515
510
[2, 3, 8, 5, 7, 3, 1, 6]
Output Number (1 2 3 4 5 6 7 8)
2 3 8 5 7 3 1 6
'select' [3..6] = [8, 5, 7, 3]
520

FIG. 5

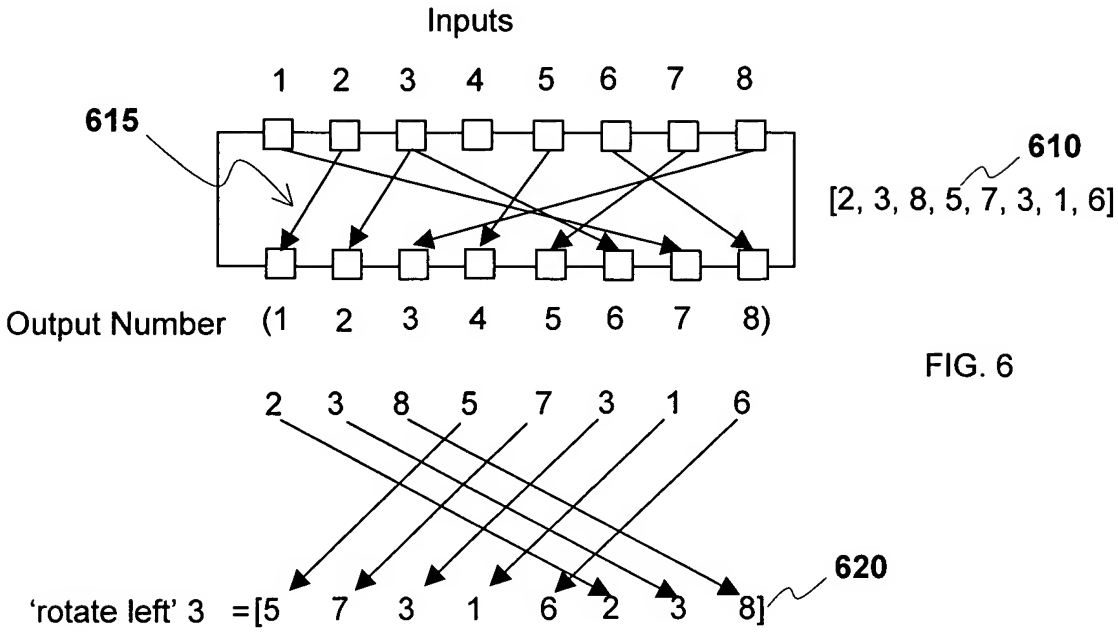

Inputs
1 2 3 4 5 6 7 8
615
610
[2, 3, 8, 5, 7, 3, 1, 6]
Output Number (1 2 3 4 5 6 7 8)

FIG. 6

2 3 8 5 7 3 1 6
620
'rotate left' 3 =[5 7 3 1 6 2 3 8]

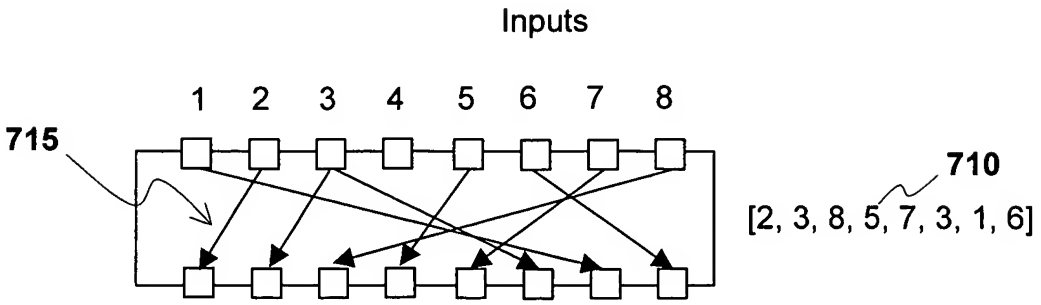
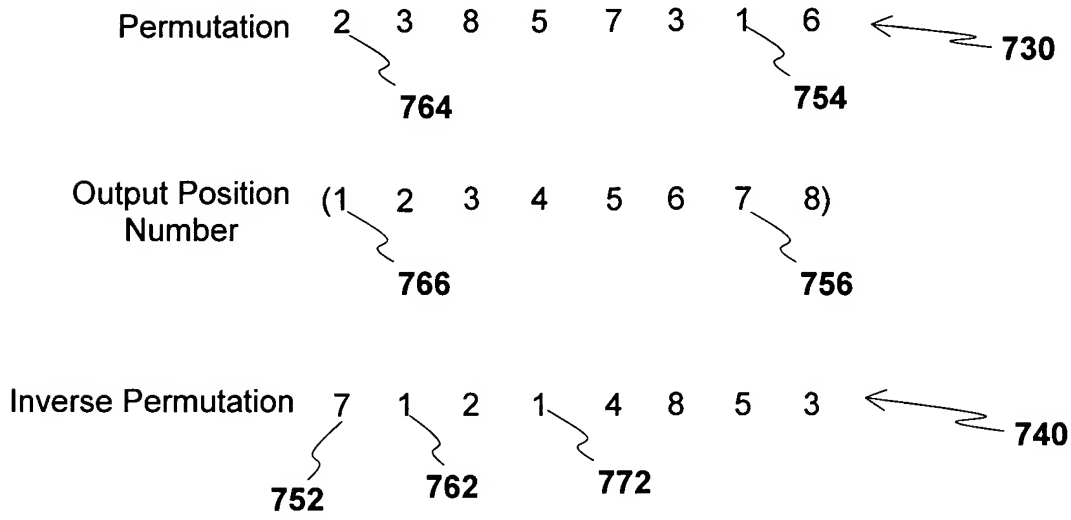

Inputs
1 2 3 4 5 6 7 8
715
710
[2, 3, 8, 5, 7, 3, 1, 6]

FIG. 7


Permutation 2 3 8 5 7 3 1 6
730
764
754
Output Position Number (1 2 3 4 5 6 7 8)
766
756
Inverse Permutation 7 1 2 1 4 8 5 3
740
752
762
772

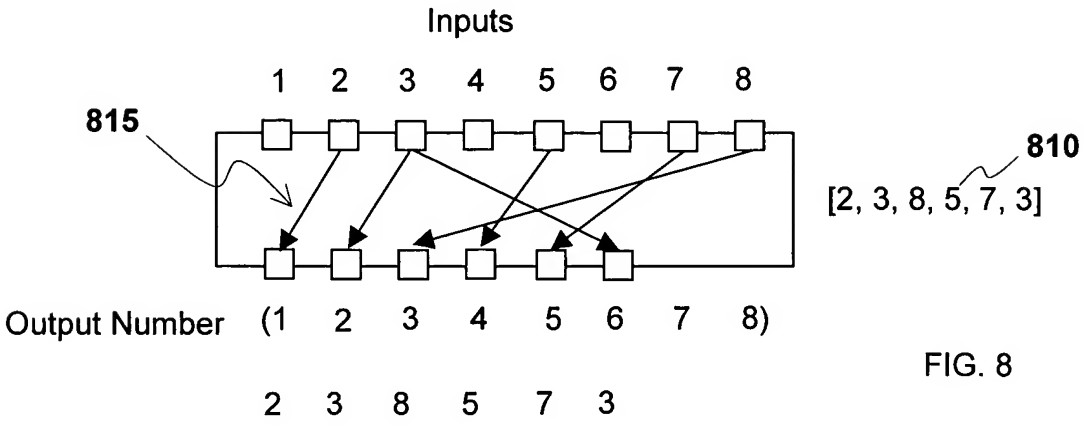
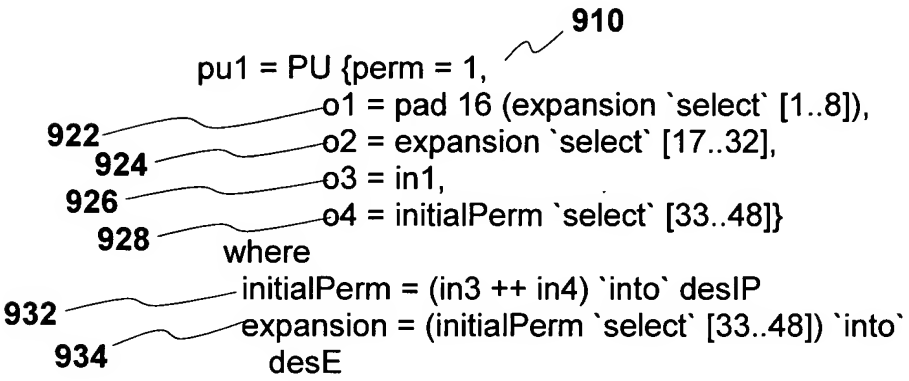


FIG. 8

pad 8 [2, 3, 8, 5, 7, 3] = [1, 1, 2, 3, 8, 5, 7, 3]

842 844




```
desE  = [32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9,
     8, 9,10,11,12,13,12,13,14,15,16,1]
```

FIG. 9

```
PU{perm=1,
    O1=[1,1,1,1,1,1,1,1,71,121,113,105,97,89,97,89],
    O2=[99,91,99,91,83,75,67,125,67,125,117,109,101,93,101,93],
    O3=[1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16],
    O4=[125,117,109,101,93,85,77,69,127,119,111,103,95,87,79,71]
    }
```

FIG. 10

```
PERM1 =
        [O1_31(IN4_16),  O2_31(IN2_31),  O3_31(IN3_31),  O4_31(IN1_31),
        O1_30(IN4_25),  O2_30(IN2_30),  O3_30(IN3_30),  O4_30(IN1_30),
        O1_29(IN4_12),  O2_29(IN2_29),  O3_29(IN3_29),  O4_29(IN1_29),
        O1_28(IN4_11),  O2_28(IN2_28),  O3_28(IN3_28),  O4_28(IN1_28),
        O1_27(IN4_3),   O2_27(IN2_27),  O3_27(IN3_27),  O4_27(IN1_27),
        O1_26(IN4_20),  O2_26(IN2_26),  O3_26(IN3_26),  O4_26(IN1_26),
        O1_25(IN4_4),   O2_25(IN2_25),  O3_25(IN3_25),  O4_25(IN1_25),
        O1_24(IN4_15),  O2_24(IN2_24),  O3_24(IN3_24),  O4_24(IN1_24),
        O1_23(IN4_31),  O2_23(IN2_23),  O3_23(IN3_23),  O4_23(IN1_23),
        O1_22(IN4_17),  O2_22(IN2_22),  O3_22(IN3_22),  O4_22(IN1_22),
        O1_21(IN4_9),   O2_21(IN2_21),  O3_21(IN3_21),  O4_21(IN1_21),
        O1_20(IN4_6),   O2_20(IN2_20),  O3_20(IN3_20),  O4_20(IN1_20),
        :
        :
        O1_2(IN4_21),   O2_2(IN2_2),    O3_2(IN3_2),    O4_2(IN1_2),
        O1_1(IN4_28),   O2_1(IN2_1),    O3_1(IN3_1),    O4_1(IN1_1),
        O1_0(IN4_7),    O2_0(IN2_0),    O3_0(IN3_0),    O4_0(IN1_0)];
```

FIG. 11

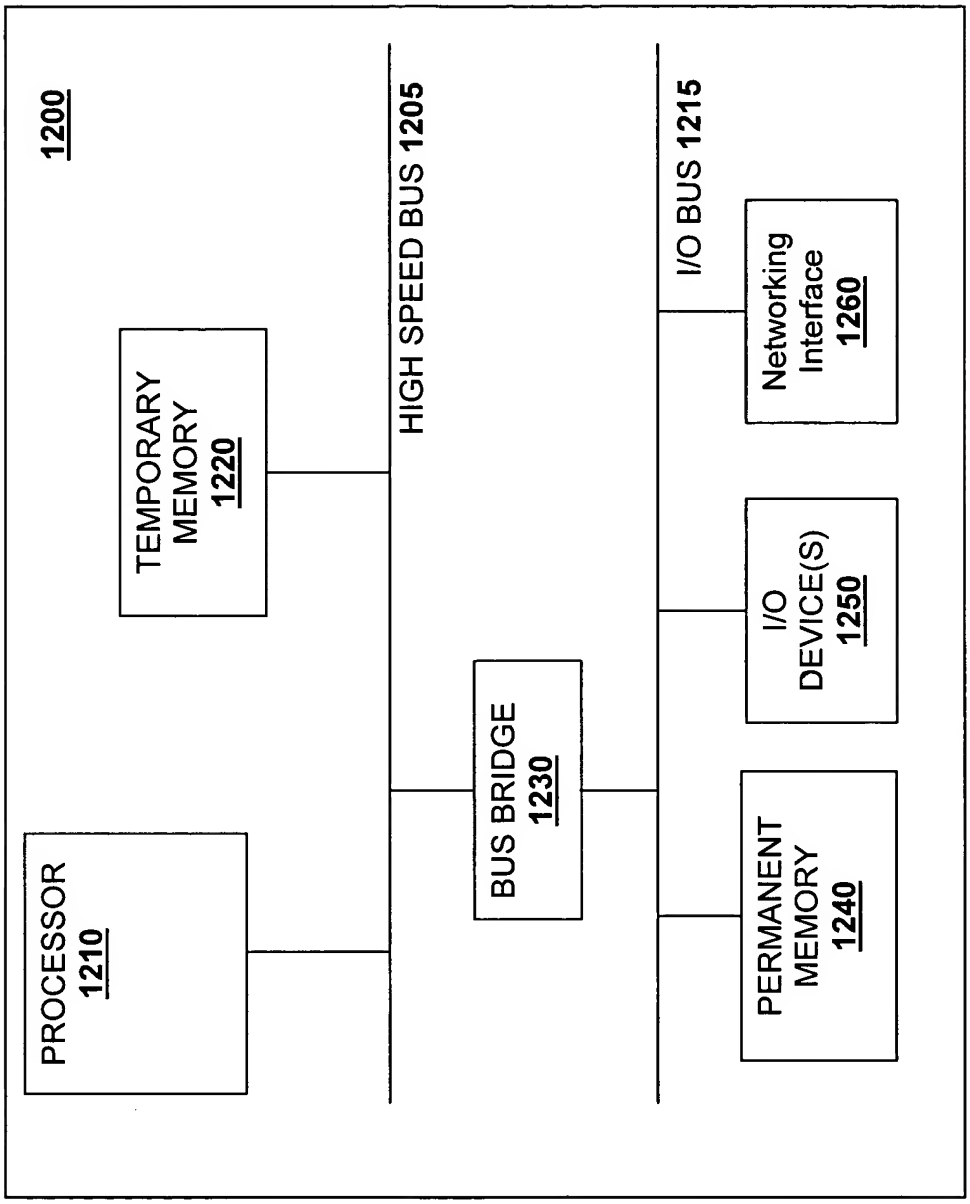

1200
PROCESSOR 1210
TEMPORARY MEMORY 1220
HIGH SPEED BUS 1205
BUS BRIDGE 1230
I/O BUS 1215
Networking Interface 1260
I/O DEVICE(S) 1250
PERMANENT MEMORY 1240

FIG. 12